STUDENT COMPUTER ACCEPTABLE USE POLICY

Drafted by:	**Assistant Head (Curriculum)**
Committee Responsible:	**School Life Sub-Committee (KD)**
Reviewed by:	**SLT and School Life Committee**
Adopted by Committee:	**March 2017**
Last reviewed:	**February 2017**

NB: Merging with E-Safety Policy – due for full review May 2021

Student Computer Acceptable Use Policy

Introduction

The use of the latest technology is actively encouraged at Sibford School but with this comes a responsibility to protect both students and the school from abuse of the system.

All students, therefore, must adhere to the policy set out below. This policy covers all computers, laptops and electronic devices within the school used during the school day or in the boarding houses, irrespective of who owns the device.

All students are expected to behave responsibly on the school computer network, as they would in classrooms and in other areas of the school. Junior School pupils are not allowed to connect their personal devices to the school network. Children in EYFS have highly supervised and limited access to the school network.

The school system has appropriate firewalls and filters to prevent access to unsuitable websites. The school keeps parents updated on issues concerning online safety by sending out updates, reminders and holding parents' information evenings.

The Policy

1. Personal Safety

1) Always be extremely cautious about revealing personal details and never reveal a home address, phone number or email address to strangers.
2) Do not send anyone your credit card or bank details without checking with a teacher.
3) Always inform your teacher or another member of staff if you have received a message or have visited a website that contains inappropriate language or makes you feel uncomfortable in any way. This can also be reported to CEOP at https://ceop.police.uk/safety-centre/
4) Always be yourself and do not pretend to be anyone or anything that you are not on the Internet.
5) Do not arrange to meet with anyone you have 'met' on the Internet – people are not always who they say they are.
6) If someone makes you an offer via email or the Internet that seems too good to be true, it probably is.
7) If in doubt ask a teacher or another member of staff.
8) Remember the advice you have received in PSHE and at other times about online safety.

2. System Security

1) Do not attempt to go beyond your authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person, or accessing another person's files. Attempting to log on as staff or an ICT administrator will be dealt with severely. You are only permitted to log on as yourself.
2) Do not give your password to any other pupil – if you do and they do something wrong while logged on as you, you will be held responsible. If you suspect someone else knows your password it will need to be changed by an ICT administrator.
3) Do not make deliberate attempts to disrupt the computer system or destroy data e.g. by knowingly distributing a virus.
4) Do not alter school hardware in any way.
5) Do not tamper with or remove any cables etc that are attached to school equipment.
6) Do not misuse hardware; treat equipment with care and respect.
7) Do not attempt to connect to another student's laptop or device while at school. You are not permitted to establish your own computer network.
8) Do not eat or drink whilst using computer equipment.
9) Do not use email or the Internet during lessons unless a member of staff has given permission.

3. Inappropriate Behaviour

(All inappropriate behaviour is against school rules and will result in serious sanctions. Here, inappropriate behaviour relates to any electronic communication device.)

1) Do not use indecent, obscene, offensive or threatening language.
2) Do not post or send information that could cause damage or disruption.
3) Do not engage in personal, prejudicial or discriminatory attacks.
4) Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
5) Do not knowingly or recklessly send or post false, defamatory or malicious information about a person or about school.
6) Do not post or send private information about another person.
7) Do not use the Internet for gambling.
8) Bullying of another person either by email, online or via texts will be treated with the highest severity AND is against the law. The police may follow up any infringements or harassment.
9) Do not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people.
10) If you mistakenly access such material please inform your teacher or another member of staff immediately, or you will be held responsible.
11) If you are planning any activity which might risk breaching the Acceptable Use Policy (e.g. research into terrorism for a legitimate project), a member of staff must be informed beforehand and give permission.
12) Do not attempt to use proxy sites on the Internet.
13) Do not take a photo of another student or member of staff without their permission. NO PHOTOGRAPHS or VIDEOS may be taken of other pupils without the permission of staff and the pupil concerned. (see the Use of Pupil Names and Images Policy).

14) Do not load photos of other people to websites or social networking sites.

4. Email

1) Do not reply to spam mails as this will result in more spam. Delete all spam mails.
2) Do not open an attachment from an unknown source as it may contain a virus.
3) Do not send or forward annoying or unnecessary messages to a large number of people e.g. chain mail.

5. Plagiarism and copyright

1) Plagiarism is taking the ideas or writings of others and presenting them as your own. Do not plagiarise works that you find on the Internet or anywhere else. This could result in disqualification from exams in the case of coursework.
2) Respect copyright. Breaking copyright law occurs when you reproduce a piece of work that is protected by copyright. If you are unsure whether or not you can use a piece of work, you should request permission from the copyright owner. This includes music files and the copying of CDs etc.

6. Privacy

1) All files and emails on the system are the property of the school. As such, system administrators and staff have the right to access them if required.
2) Do not assume any email sent on the Internet is secure.
3) All network access, web browsing and emails on the school system are logged and may be routinely monitored on any computer screen without the student's knowledge.
4) If you are suspected of breaching this policy, your own personal laptop/device and mobile phone can be searched by staff and your parents will be informed.
5) The school reserves the right to randomly search the Internet for inappropriate material posted by students and to act upon it.

7. Software

1) Do not install any software on the school system.
2) Do not attempt to download programs from the Internet onto school computers.
3) Do not knowingly install spyware or any sort of hacking software or device.

8. Sanctions

1) Sanctions will vary depending on the severity of the offence, from a warning or withdrawal of Internet use, to suspension or expulsion. Any breach of the law may lead to the involvement of the police.

9. General and Best Practice

1) When printing, only print if absolutely necessary and only print one copy; ensure your name appears on every printout.
2) Always log off your computer when you have finished using it.
3) Save work regularly using sensible file names.
4) Always back up any work that is not saved onto the school network.
5) Observe health and safety guidelines when using computer equipment.
6) Be considerate and polite to other users.
7) Leave your computer and the surrounding area clean and tidy.
8) When you leave school for good ensure you save any files you wish to take with you as your account will be deleted.
9) The school aims to inform pupils about staying safe online through PSHE and visiting speakers. We help pupils become more resilient in many ways including through the Penn Resilience programme, delivered as part of the Year 7 PSHE programme.

10. Other Electronic Devices

The above policy also covers other electronic devices such as laptops and mobile phones while used at school. However, none of these devices are covered by the school's insurance and the school accepts no liability for them. All devices should be security marked and kept locked away where possible. This also includes items such as digital cameras and personal ipods etc.

1) If you wish to use your own personal laptop you can only connect via the student network service. You must use wireless connectivity – do not cable your laptop to the network.
2) Your laptop must have up to date anti virus software installed.
3) Do not attempt to use hacking tools.
4) The use of webcams is not permitted.
5) Do not use a mobile phone during lessons unless under the direction of a member of staff or to access Firefly.
6) Do not take photos or videos, using a phone, in school unless a member of staff has given permission.
7) Do not photograph or video people without their permission.
8) The use of music/video players e.g. ipods is banned during lessons unless a teacher has given permission.
9) Do not connect music/video players to the school network or school computers.

Appendix: The information sheet below is displayed in teaching rooms:

1. School is a place of work and, as such, throughout the school day electronic devices should be used for learning and not for entertainment.
2. Care should be taken to store devices safely when not in use, for example locked in a locker. The owner is responsible for the safekeeping of the device, not the school.
3. School computers are intended for work purposes only and may be used at lunch, break and prep times under the supervision of a member of staff.
4. Pupils wishing to work at lunchtime may use the Library but please remember this is a quiet working environment.
5. Headphones may only be used in class at the discretion, and with the permission, of the teacher. They must not be worn whilst walking around school or in the dining hall.
6. Stay safe online. Never reveal your home address, phone number or email to someone you have 'met' online. Do not arrange to meet up with anyone you only know through the internet. Always stop and think of the possible consequences before you send information online.
7. You must not take or use images of pupils or staff without their permission.
8. Bullying of another person by email, text or online or inappropriate comments posted will result in disciplinary action.
9. Inappropriate use of devices, software, including firewalls, the school network or Internet will be treated as a matter of misconduct.
10. Misuse of devices may result in confiscation.
11. Think before you print – be mindful of the impact of printing on the environment. Check work before printing and name your work. Make sure you know which printer you are sending work to and collect it promptly. Print only one copy.
12. Always log in with your own username and password. Do not try to use anyone else's account. Lock a computer, if inactive, or log off when finished.

13. For school purposes always use your school email account.